REMARKS/ARGUMENTS

This paper is submitted responsive to the Office Action mailed January 17, 2008. Reconsideration and further examination of the application in light of the accompanying remarks and amendments is respectfully requested.

The Office Action entered new grounds of rejection which are acknowledged. Reconsideration of these rejections is respectfully requested.

Initially, the Examiner has rejected claims 1-11 and 14-16 as obvious based upon US patent 5,657,388 to Weiss (Weiss1) in view of US patent 5,479,512 to Weiss (Weiss2).

We note that Weiss1 does not mention in the description of the invention the use of encryption. US patent number 5,657,388 (Weiss1) deals with the issues of controlling access to resources. That is, the method of Weiss1 deals with the issue of Authentication of a user who requires access to a resource. The issue of Authentication is but one issue relevant to ensuring secure communication in a faceless computer network environment. Weiss1 addresses this issue by a method which uses an identification code which changes with time. The present invention relates to a system that uses both changing identification and encryption codes to deal with the four issues of Privacy, Authentication, Integrity and Non-Repudiation.

It is suggested by the Examiner that encryption is incorporated into Weiss1 by reference to US 5,237,614 (Weiss3) and that the only feature therefore missing is the use of changing encryption codes synchronized with a server. Weiss1 references "inferring an encryption key" as per Weiss3. Weiss3 describes this process which includes the exchange of keys between the client and server (see Fig. 2, as referenced by the

Examiner, at step 52). Therefore not only do these documents combined not disclose changing encryption codes, they also do not teach the personal code generation means having its own encryption codes, which is an essential element of the present invention. In fact, incorporating Weiss3 into Weiss1 teaches away from the present invention by directing the skilled person to the transfer of encryption codes, which the present invention is deliberately avoiding.

The Examiner also asserts that it would be obvious for the skilled person to further combine Weiss2 to arrive at the invention. The Applicant submits firstly that it would not be obvious to the skilled person to make use of changing independent codes such as that mentioned in Weiss2 in combination with Weiss1 due to the fact that Weiss3 teaches the transfer of encryption codes. Further, the Applicant submits that there would be no motivation for the skilled person to look to features mentioned in Weiss2 as this document is directed at a completely different issue. Weiss2 discloses a system which is directed at performing concurrent encryption and compression (referred to as concryption) of data in order to provide an improved system relative to compression and subsequent encryption. The document does not relate to dealing generally with all of the issues of secure communication as does the present invention.

The present invention attempts to address each of the abovementioned aspects of security (Privacy, Authentication, Integrity and Non-repudiation) by a system which uses both synchronized changing encryption and identification codes. While the abovementioned cited documents deal with some of these issues, none attempt to address all. However, if a skilled

person wished to address any particular issue not covered in any given system, the usual methods of dealing with these issues would most likely be employed. That is, Privacy with SSL (Secure Socket Layer) or VPN (Virtual Private Network) methods, Authentication with passwords and/or swipe/RFID cards, Integrity with hashes and Non-repudiation with digital signatures and biometrics.

The present invention attempts to deal with each of these issues by a system including multiple changing codes which already exist at two communication ends independent of one another. That is, one code for Privacy, a second for Authentication, the time interval between changes for Integrity and the fact that the user has a 'personal' code generation means generating unique codes for Non-repudiation. The system of multiple changing codes is one in which no other momentary code other than that assigned for authentication needs to be exchanged. Once authenticated, the communication is secured by the momentary code for Privacy (the encryption code) on the premise that the receiving end should already have the decrypting code because of the prior authentication.

While elements of the invention may be know in isolation, the Applicant submits that that combination is not one which would be an obvious solution to deal with each of the issues addressed. Of particular importance is that the invention addresses each of these issues in one action in a single technology without the need to use the abovementioned known techniques. The use of a single technology to deal with these issues results in minimal complexity and computing overheads in implementation which is a significant advantage.

On the basis of the forgoing, it is submitted that each of

independent claims 1 and 14 clearly defines over the combinations of Weiss1, Weiss2 and Weiss3, and these claims are submitted to therefore be in condition for allowance. Dependent claims 2-11 and 15-16 depend from claims 1 and 14 and are likewise submitted to be in condition for allowance.

In connection with independent claims 12 and 17, these claims were rejected over the same combination as discussed above in connection with Weiss1, Weiss2 and Weiss3, and further in view of US patent 6,981,141 to Mahne et al. It is submitted, however, that these claims are patentable for the reasons set forth above in connection with independent claims 1 and 14. The citation to Mahne et al. deals with different subject matter from claims 1 and 14 and, therefore, the above-noted deficiencies of the prior art remain.

Dependent claims 13 and 18 depend from claims 12 and 17 and are likewise submitted to be in condition for allowance on the basis of the above arguments.

This paper is accompanied by authorization to charge a fee for a one month extension of time. It is believed that no other fee is due. If any such fee is due, please charge same to Deposit Account 02-0184.

Respectfully submitted,

Azman Bin H J Zahari

By /George A. Coury/
George A. Coury
Attorney for Applicant
Reg. No. 34,309
Tel: (203) 777-6628
Fax: (203) 865-0297

Date: May 19, 2008